AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ☑ Original ❒ Duplicate O

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
CYNTHIA HAZELWOOD ("SUBJECT PERSON"), who is a white female, date of birth XX/XX/1982; and Green 2013 Chevrolet Equinox with Indiana License Plate CNS491 and VIN/ 2GNALDEK1D6309199 ("SUBJECT VEHICLE").

Case No. 24-M-458 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A1 and Attachment A2.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 8-19-24 *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 8-5-24. 11:50 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

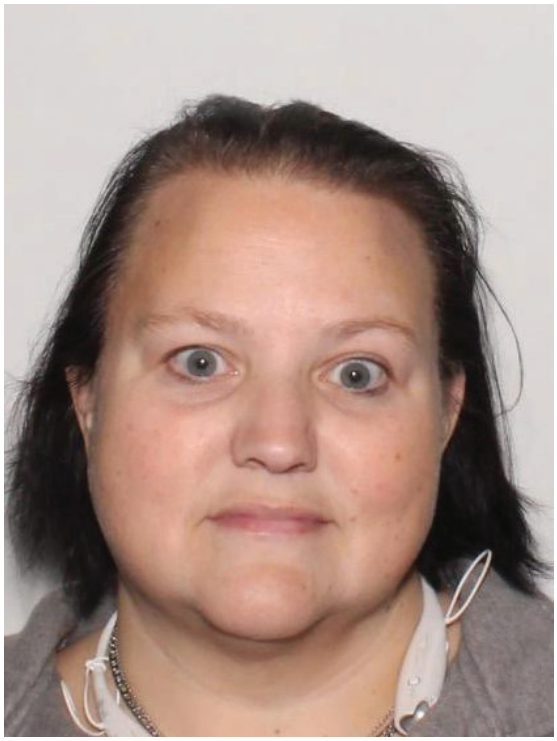
Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A1
DESCRIPTION OF PERSON TO BE SEARCHED

The person to be searched is: C**YNTHIA HAZELWOOD ("SUBJECT PERSON")**, who is a white female, date of birth XX/XX/1982 (redacted but known to Affiant), as depicted in the photograph below. Further, this search warrant authorizes the seizure and search of any portable devices (including cellular telephones) on the person of the **SUBJECT PERSON** or in her immediate reach, which are believed to belong to said person. This is to include, but not limited to, the search of any personal bags, backpacks, briefcases, and exterior clothing.



ATTACHMENT A2

DESCRIPTION OF VEHICLE TO BE SEARCHED

The vehicle to be searched is: described as identified as a **Green 2013 Chevrolet Equinox with Indiana License Plate CNS491 and VIN/ 2GNALDEK1D6309199 ("SUBJECT VEHICLE")**, registered to Cynthia Hazelwood, as depicted in the photograph below.

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations Title 18, United States Code, Sections 2251 (sexual exploitation of a minor), 2252 (certain activities relating to material involving the sexual exploitation of minors), and 2252A (certain activities relating to material constituting or containing child pornography) ("Subject Offenses"), including the following:

1. Records and information pertaining to telephone number 260-293-XXXX (redacted), "Cyndi Quality Inn", or Cory Cox;

2. Records and information pertaining to producing, transporting, advertising, shipping, distributing, receiving, or possessing child pornography or visual depictions of minors engaging in sexually explicit conduct, as defined at 18 U.S.C. § 2256(8);

3. Records and information pertaining to coercion or threats to produce pornography and/or sexually explicit images/videos;

4. Records and information showing or evidencing a sexual interest in minors or a desire or motive to collect or distribute visual depictions of minors engaged in sexually explicit conduct or child pornography, or child erotica;

5. Records and information pertaining to the transfer of obscene matter to another individual who has not attained the age of 16 years, knowing that the other person has not attained the age of 16 years;

6. Records and information pertaining to personal contact and other activities with minors visually depicted while engaged in sexually explicit conduct;

7. Records and information pertaining to telephone accounts, to include without limitation account information, telephone numbers, bills, statements, transaction history/toll logs, and payment information;

8. Records and material concerning indicia of use, ownership, possession, or control of the search locations described in **Attachments A1 and A2**, and the items located within, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

9. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of the Subject Offenses.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the search locations described in **Attachments A1 and A2** also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section A of this Attachment above, including, but not limited to, desktop and laptop computers, cellular telephones/smart phones, vehicle navigation systems,

disk drives, routers, modems, thumb drives, personal digital assistants, digital cameras, and scanners, network equipment (the "Subject Devices"). This warrant includes the search and seizure of the content contained within the Subject Devices, to include:

1. All of the records and information described in Part A above;

2. Evidence of who used, owned, or controlled the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

3. Evidence indicating how and when the Subject Devices were accessed or used to determine the chronological context of device access, use, and events relating to crime under investigation and to the device user;

4. Evidence indicating the Subject Device user's state of mind as it relates to the crime under investigation;

5. Evidence of software that would allow others to control the Subject Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

6. Evidence of the lack of such malicious software;

7. Evidence of the attachment to the Subject Devices of other storage devices or similar containers for electronic evidence;

8. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Devices;

9. Evidence of the times the Subject Devices was used;

10. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Devices;

11. Documentation and manuals that may be necessary to access the Subject Devices or to conduct a forensic examination of the Subject Devices;

12. Records of or information about Internet Protocol addresses used by the Subject Devices (including port numbers);

13. Records of or information about the Subject Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

14. All location history associated with the Subject Device (including GPS, vehicle navigation, and/or any other location data);

15. Contextual information necessary to understand the evidence described in this attachment.

In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any

mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

C. Biometrics

During the execution of the search of the locations described in Attachments A1 and A2, law enforcement personnel are also specifically authorized to compel **CYNTHIA HAZELWOOD (the SUBJECT PERSON)** to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the devices found at the search locations described in Attachments A1 and A2, and

b. where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the devices' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the search locations described in Attachments A1 and A2 to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device. Further, this warrant does not authorize law enforcement personnel to request that the **SUBJECT PERSON** state or otherwise provide the password or any other means that may be used to unlock or access the

devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

CYNTHIA HAZELWOOD ("SUBJECT PERSON"), who is a white female, date of birth XX/XX/1982; and Green 2013 Chevrolet Equinox with Indiana License Plate CNS491 and VIN/ 2GNALDEK1D6309199 ("SUBJECT VEHICLE").

Case No. 24-M-458 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A1 and Attachment A2.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251	sexual exploitation of a minor
18 U.S.C. § 2252	certain activities relating to material involving the sexual exploitation of minors
18 U.S.C. § 2252(A)	certain activities relating to material constituting or containing child pornography

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Laura Smith
Digitally signed by Laura Smith
Date: 2024.08.02 13:05:30 -04'00'

Applicant's signature

Laura Smith, Task Force Officer - USSS

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 8-5-24

Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANTS

I, Laura Smith, Task Force Officer, United States Secret Service ("USSS"), being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. **Affiant**: I am a Task Force Officer with the USSS and a Detective in the Cybercrime Unit of the Indianapolis Metropolitan Police Department. I have over 26 years of law enforcement experience. I have investigated State and Federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have written numerous search warrants involving internet crimes against children cases and participated in their execution. I have attended and presented at the National Crimes Against Children Conference multiple times and attended numerous classes related to investigating the online sexual exploitation of children. I am also a member of the Indiana Internet Crimes Against Children Task Force, which includes numerous federal, state, and local law enforcement agencies. I am currently assigned to operate in an undercover capacity on the Internet to identify and investigate persons attempting to exploit or solicit sexual acts with children or trafficking in child pornography. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, 2252A, 2242, and 2243, and I am authorized by law to request

a search warrant.

2. **Requested Action:** I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to search the following:

A. The person of **Cynthia Hazelwood ("SUBJECT PERSON")** (described further in Attachment A1, attached hereto and incorporated herein); and

B. The vehicle described as a **2013 Green Chevrolet Equinox with Indiana License Plate #CNS491 ("SUBJECT VEHICLE")**, registered to Cynthia Hazelwood (described further in Attachment A2, attached hereto and incorporated herein);

(collectively described in Attachment A) for the seizure of the items more particularly described in Attachment B (attached hereto an incorporated herein), including the seizure and search of any computers, cellular telephones, and/or any other electronic devices located within (including the data contained therein), as evidence, contraband, fruits, and instrumentalities of violations or attempted violations of the following offenses, Title 18, United States Code, Sections 2251 (sexual exploitation of a minor), 2252 (certain activities relating to material involving the sexual exploitation of minors), and 2252A (certain activities relating to material constituting or containing child pornography) (the "Subject Offenses"), which items are more specifically described in Attachment B of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about

this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Task Force Officer. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations or attempted violations of the Subject Offenses are presently located on the **SUBJECT PERSON** and within the **SUBJECT VEHICLE**.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2251(a) and (e) prohibit any person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or having a minor assist any other person to engage in, or transporting any minor in or affecting interstate or foreign commerce with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility

of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed; or if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer; or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed; or attempting or conspiring to do so.

b. 18 U.S.C. § 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting

interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

e. 18 U.S.C. § 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

f. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child

pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

g. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not

necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer software," as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

j. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

m. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

n. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

o. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

s. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

t. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, thumb drives, SD/Micro SD cards, and other magnetic or optical media.

u. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

v. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable

of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

w. "Webcam," as used herein, refers to a video camera that attaches to a computer or that is built into a laptop or desktop screen. It is widely used for video calling as well as to continuously monitor an activity and send it to a Web server for public or private viewing. Webcams generally have a microphone built into the unit or use the computer's microphone for audio.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. Based on my training and experience, and the facts as set forth below in this Affidavit, there is probable cause to believe that the **SUBJECT PERSON** DOB XX-XX-1982 (known to Affiant, but redacted), has committed the following offenses in the Southern District of Indiana and elsewhere, and that evidence and/or instrumentalities of these offenses are located at the search locations described herein. This Affiant learned the following information:

7. During November 2023, I received a Cybertip from the National Center for Missing and Exploited Children (NCMEC) regarding an individual who was suspected of uploading child pornography to Dropbox. I identified Cory Cox as the target of that investigation. On or about March 19, 2024, a federal grand jury sitting in Indianapolis, Indiana returned an indictment against Cory Cox under Cause Number 1:24-cr-00047-TWP-MJD, for receiving, distributing, and possessing child pornography, in violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1), and 2252A(a)(5)(B) and (b)(2).

8. As part of that investigation into Cory Cox, on or about December 5, 2023, I obtained a search warrant for Cory Cox's person, which authorized the seizure and search of any portable devices on his person or in his immediate reach. The search warrant was granted by Marion County under cause #49D-36-2312-MC-033883.

9. After checking locations frequented by Cory Cox, Lt. Baker of Fishers Police Department spoke with Hamilton County Sex Offender Registry. He learned that Cox routinely checked-in at the Hamilton County Adult Detention Center on Wednesdays.

10. On December 6, 2023, I, along with other units, met at the Hamilton County Adult Detention Center and was notified at 9:54 a.m. that Cox had checked in. After detaining Cox in the lobby, he was searched pursuant to the Marion County search warrant. Detectives located two cellular phones on his person – one of which was a Samsung Galaxy.

11. At approximately 10:00 a.m. I read the Indiana advice of rights Miranda document to Cox. The interview was audio and video recorded. Cox said that he understood his rights and signed the document. During the course of that interview, Cox was asked about the Samsung phone. He said it was a WIFI only phone and that his sister, who resides in Florida, has autopay on for the phone service.

12. The phones were transported by Lt. Baker of Fishers PD to Hamilton County ICAC office at Fishers PD.

13. I reviewed the forensic examination report of Cox's Samsung phone.

There was a significant amount of attribution evidence on the phone showing that Cory Cox was the user of the device.

14. Amongst other things, I located chats between Cory Cox and a contact identified as "Cyndi Quality Inn" with phone number 260-293-XXXX (redacted, but known to this Affiant). The text messages were between on or about November 24, 2023 and on or about December 6, 2023.

a. On or about November 28, 2023, at 4:39 PM, "Cyndi Quality Inn" (260-293-XXXX) (redacted) sent a file entitled **PART_1701725578618** to Cory Cox. I reviewed that image file, which depicts a prepubescent female minor with her genitals exposed.

b. On or about November 28, 2023, at 7:17 PM, Cory Cox sent a file entitled **PART_1701771993108** to Cyndi Quality Inn. I reviewed that images file, which depicts an adult male engaging in sexually explicit conduct with a prepubescent female minor, placing his mouth on her exposed genitals.

c. Through my training and experience, this Affiant believes these images and video constitute child pornography as defined in 18 U.S.C. § 2556(8).

15. I requested a federal grand jury subpoena for Verizon account records relating to telephone number 260-293-XXXX (redacted).

16. On March 20, 2024, Verizon provided the subscriber as "Donald Siples" of Wolcottville, Indiana. An open-source search of Donald Siples revealed a Facebook page (https://www.facebook.com/donald.siples.XX (redacted). I reviewed the publicly

available portion of the Facebook page and observed the following female depicted in an image on that page:

17. I believe this image depicts a female whose similar image was also within the chat between Cory Cox and "Cyndi Quality Inn" as follows:

18. This female in the photograph on the "Donald Siples" Facebook page was linked to the Facebook page as https://www.facebook.com/cyndi.swift20XX (redacted). I reviewed the publicly available portion of that Facebook page and observed that her vanity name was listed as "Cyndi Hazelwood".

19. With this information, I queried the name Cynthia Hazelwood through the Indiana Bureau of Motor Vehicles (BMV) and located a **Cynthia Hazelwood**

(SUBJECT PERSON), date of birth XX-XX-1982 (known to Affiant but redacted) with an address listed in Noblesville, Indiana.

20. I requested additional information from Julia Zorger, an analyst with the Indiana State Police. She provided information that the **SUBJECT PERSON** has a current vehicle registration as of February 20, 2024, with the address at the Quality Inn as follows: 17070 Dragonfly Drive, Noblesville, Indiana 46060 Quality Inn, Unit 121. The vehicle is a **2013 Green Chevrolet Equinox with Indiana License Plate #CNS491 (SUBJECT VEHICLE)**. A query of the **SUBJECT VEHICLE** through the Indiana BMV revealed the VIN as 2GNALDEK1D6309199.

21. On July 10, 2024, this affiant reviewed data from a license plate recognition software utilized by law enforcement that provides data on when and where a specific license plate is recognized by one of its cameras, with respect to the license plate associated with the **SUBJECT VEHICLE**.

22. Between June 18, 2024, and July 22, 2024, the license plate belonging to the **SUBJECT VEHICLE** was located in numerous cities and counties in Indiana, Illinois, and Wisconsin. Specifically, the **SUBJECT VEHICLE** was identified in the following cities and counties on the corresponding dates:

a. **June 18, 2024:** LaGrange County, IN

b. **June 19, 2024:** Muncie, IN

c. **June 20, 2024:** Anderson, IN; Fishers, IN; Noblesville, IN; Lapel, IN; and Chesterfield, IN

d. **June 22, 2024:** Wells County, IN

e. **June 28, 2024:** Marshall County, IN; Starke County, IN; Porter County, IN; and Gary, IN

f. **July 9, 2024:** Lombard, IL; and Dupage County, IL

g. **July 22, 2024:** Greenfield, WI

23. This Affiant requested and received a search warrant in the United States District Court for the Southern District of Indiana under Cause Number 1:24-mj-00672-TAB to obtain records and information regarding the location of the cell phone with the number 260-293-XXXX (redacted, but known to this Affiant), utilized by the **SUBJECT PERSON.**

24. The information received in response to that search warrant indicates that the cell phone with the number 260-293-XXXX (redacted, but known to this Affiant), utilized by the **SUBJECT PERSON**, has been located in and around Milwaukee, Wisconsin, between July 27 and August 1, 2024.

25. On July 27, 2024, at 11:12 AM (UTC), the device was located near 829 Grandstand Avenue, West Allis, Wisconsin. This is located inside the area of the Wisconsin State Fair Park.

26. On July 28, 2024, at 5:28 AM (UTC), the device was located near the area of 829 Grandstand Avenue.

27. On July 29, 2024, at 5:42 AM (UTC), the device was located near S. 76th Street and W. Kearney Street, Milwaukee, WI. This location is identified from Google maps as the WisDOT State Fairgrounds Park & Ride. On the same date at 7:12 AM (UTC) the device was still at this location. At 9:12 AM (UTC) the device was located

also in the same area near 829 Grandstand Avenue, West Allis, Wisconsin.

28. This Affiant believes, based on that location data, that the **SUBJECT PERSON** is staying at the Wisconsin State Fair Grounds located at 640 S. 84th Street in West Allis, Wisconsin.

29. This Affiant knows that persons who have sexually exploited minors and/or are sexually attracted to children will rarely, if ever, dispose of their collections even when they move from one residence to another.

30. Additionally, this affiant knows that persons who collect sexually explicit images of minors usually maintain their collections on multiple devices and multiple social media and/or cloud-based platforms. They typically maintain their collections close by, where they can have near immediate access to them, such as on their person, in their homes/property, and/or vehicles.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

31. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting

the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and

carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN OR WHO PRODUCE, RECEIVE, AND/OR POSSESS CHILD PORNOGRAPHY

32. Based on my previous investigative experience related to child-exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices

through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the individual uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found on the individual's person and/or inside the individual's vehicle, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

1 *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

33. Based on all of the information contained herein, I believe that the **SUBJECT PERSON** likely displays characteristics common to individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

34. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PERSON** and/or **SUBJECT VEHICLE**, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

35. I submit that if a computer or storage medium is found on the **SUBJECT PERSON** or in the **SUBJECT VEHICLE**, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

36. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There

is probable cause to believe that this forensic electronic evidence will be on any storage medium on the **SUBJECT PERSON** or in the **SUBJECT VEHICLE** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet

history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or

exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of

counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

37. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg"

often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

38. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet

and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

39. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

40. This warrant permits law enforcement to compel **CYNTHIA HAZELWOOD (the SUBJECT PERSON)** to unlock any electronic devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or

alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through their fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through their face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of their face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with their irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers their irises by holding the device in front of their face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of the **SUBJECT PERSON** to the fingerprint scanner of the devices found on the **SUBJECT PERSON** or within the **SUBJECT VEHICLE** (as described in Attachment A); and (2) hold those devices in front of the face of the **SUBJECT PERSON** and activate the facial recognition feature, for the purpose of attempting

to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that the **SUBJECT PERSON** state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel the **SUBJECT PERSON** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

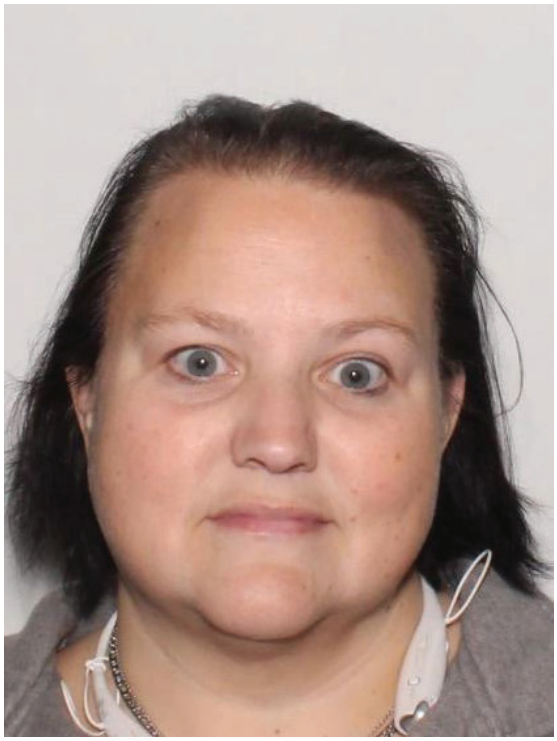
41. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A: the **SUBJECT PERSON** and **SUBJECT VEHICLE**. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

42. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

I swear under penalty of perjury that the foregoing is true.

ATTACHMENT A1
DESCRIPTION OF PERSON TO BE SEARCHED

The person to be searched is: C**YNTHIA HAZELWOOD ("SUBJECT PERSON")**, who is a white female, date of birth XX/XX/1982 (redacted but known to Affiant), as depicted in the photograph below. Further, this search warrant authorizes the seizure and search of any portable devices (including cellular telephones) on the person of the **SUBJECT PERSON** or in her immediate reach, which are believed to belong to said person. This is to include, but not limited to, the search of any personal bags, backpacks, briefcases, and exterior clothing.



ATTACHMENT A2

DESCRIPTION OF VEHICLE TO BE SEARCHED

The vehicle to be searched is: described as identified as a **Green 2013 Chevrolet Equinox with Indiana License Plate CNS491 and VIN/ 2GNALDEK1D6309199 ("SUBJECT VEHICLE")**, registered to Cynthia Hazelwood, as depicted in the photograph below.

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations Title 18, United States Code, Sections 2251 (sexual exploitation of a minor), 2252 (certain activities relating to material involving the sexual exploitation of minors), and 2252A (certain activities relating to material constituting or containing child pornography) ("Subject Offenses"), including the following:

1. Records and information pertaining to telephone number 260-293-XXXX (redacted), "Cyndi Quality Inn", or Cory Cox;

2. Records and information pertaining to producing, transporting, advertising, shipping, distributing, receiving, or possessing child pornography or visual depictions of minors engaging in sexually explicit conduct, as defined at 18 U.S.C. § 2256(8);

3. Records and information pertaining to coercion or threats to produce pornography and/or sexually explicit images/videos;

4. Records and information showing or evidencing a sexual interest in minors or a desire or motive to collect or distribute visual depictions of minors engaged in sexually explicit conduct or child pornography, or child erotica;

5. Records and information pertaining to the transfer of obscene matter to another individual who has not attained the age of 16 years, knowing that the other person has not attained the age of 16 years;

6. Records and information pertaining to personal contact and other activities with minors visually depicted while engaged in sexually explicit conduct;

7. Records and information pertaining to telephone accounts, to include without limitation account information, telephone numbers, bills, statements, transaction history/toll logs, and payment information;

8. Records and material concerning indicia of use, ownership, possession, or control of the search locations described in **Attachments A1 and A2**, and the items located within, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

9. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of the Subject Offenses.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the search locations described in **Attachments A1 and A2** also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section A of this Attachment above, including, but not limited to, desktop and laptop computers, cellular telephones/smart phones, vehicle navigation systems,

disk drives, routers, modems, thumb drives, personal digital assistants, digital cameras, and scanners, network equipment (the "Subject Devices"). This warrant includes the search and seizure of the content contained within the Subject Devices, to include:

1. All of the records and information described in Part A above;

2. Evidence of who used, owned, or controlled the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

3. Evidence indicating how and when the Subject Devices were accessed or used to determine the chronological context of device access, use, and events relating to crime under investigation and to the device user;

4. Evidence indicating the Subject Device user's state of mind as it relates to the crime under investigation;

5. Evidence of software that would allow others to control the Subject Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

6. Evidence of the lack of such malicious software;

7. Evidence of the attachment to the Subject Devices of other storage devices or similar containers for electronic evidence;

8. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Devices;

9. Evidence of the times the Subject Devices was used;

10. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Devices;

11. Documentation and manuals that may be necessary to access the Subject Devices or to conduct a forensic examination of the Subject Devices;

12. Records of or information about Internet Protocol addresses used by the Subject Devices (including port numbers);

13. Records of or information about the Subject Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

14. All location history associated with the Subject Device (including GPS, vehicle navigation, and/or any other location data);

15. Contextual information necessary to understand the evidence described in this attachment.

In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any

mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

C. Biometrics

During the execution of the search of the locations described in Attachments A1 and A2, law enforcement personnel are also specifically authorized to compel **CYNTHIA HAZELWOOD (the SUBJECT PERSON)** to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the devices found at the search locations described in Attachments A1 and A2, and

b. where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the devices' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the search locations described in Attachments A1 and A2 to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device. Further, this warrant does not authorize law enforcement personnel to request that the **SUBJECT PERSON** state or otherwise provide the password or any other means that may be used to unlock or access the

devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.